○警察情報セキュリティ管理要綱

平成26年３月27日

情管第７９５号

警察本部長

警察情報セキュリティ管理要綱の制定について（通達）

この度、情報セキュリティをめぐる情勢の変化等を踏まえ、埼玉県警察における警察情報セキュリティの管理に関し、みだしの要綱を別添のとおり制定し、平成26年４月１日から実施することとしたので、誤りのないようにされたい。

なお、警察情報セキュリティ対策基準（平成23年情管第2546号）は、平成26年３月31日限り、廃止する。

別添

警察情報セキュリティ管理要綱

第１　総則

１　趣旨

この要綱は、警察情報セキュリティに関する規程（平成19年埼玉県警察本部訓令第40号。以下「セキュリティ訓令」という。）第３条第２項及び第８条第２項の規定に基づき、警察情報セキュリティを確保するために必要な管理体制を定めるものとする。

２　情報の分類

セキュリティ訓令第８条第１項の情報の分類は、次のとおりとする。

(1)　機密性

ア　機密性高　情報のうち、秘密文書（埼玉県警察文書管理規程（平成14年埼玉県警察本部訓令第25号）第48条に定めるものをいう。）の内容に相当する情報その他の機密性が損なわれることによる影響が大きいもの

イ　機密性中　情報のうち、直ちに一般に公開することを前提としていないもの

ウ　機密性低　情報のうち、機密性高又は中に分類される情報以外のもの

(2)　完全性

ア　完全性高　情報のうち、改ざんされ、又は滅失した場合に業務の的確な遂行に支障を及ぼすおそれがあるもの

イ　完全性低　情報のうち、完全性高に分類される情報以外のもの

(3)　可用性

ア　可用性高　情報のうち、その情報が使用できないときに業務の安定的な遂行に支障を及ぼすおそれがあるもの

イ　可用性低　情報のうち、可用性高に分類される情報以外のもの

３　定義

この要綱において使用する用語は、セキュリティ訓令において使用する用語の例によるほか、次に掲げる用語の意義は、それぞれ定めるところによる。

(1)　警察情報セキュリティポリシー　セキュリティ訓令及びセキュリティ訓令に基づき定められた情報セキュリティに関する事項をいう。

(2)　要機密情報　機密性高又は中に分類される情報をいう。

(3)　アクセス　警察情報システムにデータを入力し、又は警察情報システムからデータを出力することをいう。

(4)　ＩＤ　アクセス権者を識別するために、アクセス権者ごとに重複せずに付与された文字列をいう。

(5)　パスワード　警察情報システムを利用しようとする者がアクセス権者本人であるかを検証するために用いられる文字列をいう。

(6)　認証　ＩＤ、パスワード等を警察情報システムに入力することなどにより、アクセスを行う者が正当な者であるか否かを検証することをいう。

(7)　入出力資料　警察情報システムに入力され、又は警察情報システムにより出力された情報を記録した文書、図画及び電磁的記録（作成中のものを含む。）をいう。

(8)　ドキュメント　警察情報システムに関する次に掲げる文書、図画及び電磁的記録（作成中のものを含む。）をいう。

ア　システムドキュメント

(ｱ)　システム仕様書

(ｲ)　システム設計書（情報の処理の手順並びに機器及びプログラムの構成の概要の記録をいう。）

(ｳ)　プログラム仕様書（情報処理の手順の概要の記録をいう。）

(ｴ)　プログラムリスト

(ｵ)　操作指示書（システムの維持管理に伴う機器の設定方法を説明した記録をいう。）

イ　取扱説明書　警察情報システムを利用する者が業務を行う上で参照する機器の操作の方法を説明した記録をいう。

(9)　外部記録媒体　フロッピーディスク、フラッシュメモリ、ＤＶＤ規格媒体等電子計算機に接続し、情報を入出力する電磁的記録媒体をいう。

(10)　ネットワーク機器　システムを構成するルータ、ハブ等の機器又はこれらから出力されるデータを利用することによりネットワークを管理する機能を有する機器をいう。

(11)　外部回線　警察の管理が及ばない電子計算機が論理的に接続され、当該電子計算機の通信に利用されるインターネットその他の電気通信回線をいう。

(12)　電子計算機　コンピュータ全般のことを指し、オペレーティングシステム及び接続された周辺機器を含むサーバ等及び端末装置をいう。

(13)　ネットワーク端末　ネットワークを介して他の電子計算機と接続された端末装置であって、インターネットに接続されていないものをいう。

(14)　インターネット端末　インターネットに接続された端末装置をいう。

(15)　スタンドアロン電子計算機　他の電子計算機と接続されていない電子計算機をいう。

(16)　モバイル端末　一の警察の庁舎内から移動して運用するものとして整備した電子計算機（携帯電話機（スマートフォンを含む。）を含む。）をいう。

(17)　サーバ等　情報を体系的に記録し、検索し、又は編集する機能を有するサーバ及び汎用電子計算機をいう。

(18)　自己復号型暗号　特定のソフトウェアをインストールすることなく復号することのできる暗号をいう。

(19)　情報セキュリティインシデント　情報セキュリティの維持を困難とする事案をいう。

第２　情報セキュリティ委員会の構成等

１　構成

(1)　セキュリティ訓令第３条の情報セキュリティ委員会（以下「委員会」という。）は、委員長、副委員長及び委員をもって構成する。

(2)　委員長は警察本部長、副委員長は総務部長をもって充てる。

(3)　委員は、警務部長、生活安全部長、地域部長、刑事部長、交通部長、警備部長、さいたま市警察部長、警察学校長及び各方面本部長並びに関東管区警察局埼玉県情報通信部長をもって充てる。

２　任務

委員会の任務は、次に掲げる事項の審議とする。

(1)　警察情報システムにおいて取り扱われる各種対策の基準

(2)　警察情報システムに係る情報セキュリティが侵害された場合の再発防止計画

(3)　その他警察情報システムに係る情報セキュリティに関する事項で、委員長が重要と認めるもの

３　専門部会

(1)　委員会に、委員長から付託された警察情報システムに係る情報セキュリティに関する事項を調査し、又は審議するため、情報セキュリティ専門部会（以下「専門部会」という。）を置く。

(2)　専門部会は、部会長、副部会長及び部会員をもって構成する。

(3)　部会長は総務部長、副部会長は総務部情報管理課長（以下「情報管理課長」という。）をもって充てる。

(4)　部会員は、総務部総務課長、同部財務局会計課長、警務部警務課長、生活安全部生活安全企画課長、地域部地域課長、刑事部刑事総務課長、交通部交通企画課長及び警備部公安第一課長並びに第一方面本部副本部長並びに警察学校副校長並びに総務部情報管理課情報セキュリティ対策室長及び警務部警務課企画調整室長並びに関東管区警察局埼玉県情報通信部通信庶務課長をもって充てる。

(5)　部会長は、専門部会の調査又は審議状況を委員会に報告するものとする。

4　分科会

(1)　専門部会に、特定の事項を調査し、又は研究するため、情報セキュリティ分科会（以下「分科会」という。）を置く。

(2)　分科会に分科会長を置き、情報管理課長をもって充てる。

(3)　分科会は、分科会長が指定する者をもって組織する。

5　運営

(1)　委員会、専門部会及び分科会の会議は、各会の長が必要に応じて招集し、議事を主宰する。

(2)　各会の長は、必要があると認めるときは、定められた構成員以外の者に対し各会への出席を求めることができる。

(3)　前記(1)及び(2)に規定するもののほか、委員会、専門部会及び分科会の運営に関し必要な事項は、各会の長が定める。

6　庶務

委員会、専門部会及び分科会の庶務は、総務部情報管理課において処理する。

第３　情報セキュリティ管理者の遵守事項

セキュリティ訓令第４条の情報セキュリティ管理者が遵守すべき事項は、次のとおりである。

(1)　情報セキュリティ管理者は、情報セキュリティに係る事務を総括整理するに当たっては、その事務に関係するシステムセキュリティ責任者（第５の１に規定する者をいう。）及びシステムセキュリティ維持管理者（第６の１に規定する者をいう。）の意見を聴き、十分検討した上で処理しなければならない。

(2)　情報セキュリティ管理者は、警察情報システムについて一元的に把握し管理するため、必要な事項を記載した台帳を整備しなければならない。

(3)　情報セキュリティ管理者は、職員に警察情報セキュリティポリシーを正しく理解させ、確実に遵守させるため、職員の職務に応じた教養を実施しなければならない。

(4)　情報セキュリティ管理者は、災害時等において、警察情報システムの復旧、通信手段の確保等のためにやむを得ないときは、警察情報セキュリティポリシーの規定にかかわらず、所要の措置をとるものとする。

第４　区域情報セキュリティ管理者

１　区域情報セキュリティ管理者の設置

(1)　情報セキュリティ管理者は、それぞれの庁舎の敷地を複数の区域に分割し、当該区域をクラス０からクラス３までに分類する。

(2)　クラス０の区域を除く各区域に区域情報セキュリティ管理者を置く。

(3)　区域の分類及び区域情報セキュリティ管理者は次の基準による。

ア　クラス０

各庁舎の敷地内であって、職員以外の者が自由に立ち入ることのできる区域は、一の区域とし、クラス０に分類する。

イ　クラス１

各庁舎における廊下等、職員の共用の区域は、一の区域とし、クラス１に分類するとともに、区域情報セキュリティ管理者に、当該庁舎の庁舎管理に関する事務を処理する者をもって充てる。

ウ　クラス２

執務室は、所属ごとに一の区域とし、クラス２に分類するとともに、区域情報セキュリティ管理者に、各所属の長をもって充てる。

エ　クラス３

警察情報システムに係る機械室は、室ごとに一の区域とし、クラス３に分類するとともに、区域情報セキュリティ管理者に、当該機械室を管理する所属の長をもって充てる。

2　区域情報セキュリティ管理者の責務

区域情報セキュリティ管理者は、当該区域における情報セキュリティの確保のための管理対策を行うものとする。

3　区域情報セキュリティ管理者の遵守事項

区域情報セキュリティ管理者は、関係する他の区域情報セキュリティ管理者、情報セキュリティ管理者等と連携し、次に定める対策を実施しなければならない。

(1)　クラス１の管理対策

ア　職員以外の者が不正に立ち入ることがないよう対策をとらなければならない。

イ　職員以外の者を立ち入らせるときは、その者の氏名、所属、訪問目的及び訪問相手を確認しなければならない。ただし、継続的に立入りを許可された者にあっては、この限りでない。

ウ　職員以外の者を立ち入らせるときは、職員とは種別の異なるカードを身に付けさせるなどして、職員とそれ以外の者を視覚上区別できるようにしなければならない。

(2)　クラス２の管理対策

ア　下位区域との境界を施錠可能な扉等によって仕切らなければならない。

イ　無人となるときは施錠しなければならない。

ウ　職員以外の者を立ち入らせるときは、当該区域内に設置された電子計算機の画面を不正に視認されないよう留意しなければならない。

エ　クラス０に分類される区域と接するときは、当該境界において前記(1)に定める対策を実施しなければならない。ただし、合同庁舎等において、他の機関が前記(1)と同等以上の対策を実施しているときは、この限りでない。

(3)　クラス３の管理対策

ア　常時施錠し、立ち入ることができる者の名簿を作成しなければならない。名簿に記載された者以外の者が立ち入る必要があるときは、区域情報セキュリティ管理者の承認を得させなければならない。

イ　当該区域に立ち入る者の氏名及びその入退室の時刻を記録しなければならない。この場合において、当該記録は、可能な限り電磁的に記録させなければならない。

ウ　電子計算機の画面、システムドキュメント及び入出力資料をその区域の外から視認することができない構造としなければならない。

エ　職員以外の者が立ち入っている間は、職員が立ち会わなければならない。

オ　自然災害の発生等を原因とする情報セキュリティの侵害に対して、施設及び環境面から対策を講じなければならない。

4　例外

情報セキュリティ管理者が、前記１(3)の基準による運用を困難と認めたときは、当該基準によらない区域を別に定めることができる。この場合において、情報セキュリティ管理者は、前記３の規定を参考として、関係する他の情報セキュリティ管理者等と連携の上、可能な限り情報セキュリティの確保のための管理対策を行わなければならない。

第５　システムセキュリティ責任者

１　システムセキュリティ責任者の設置

警察情報システムの整備を担当する所属にシステムセキュリティ責任者を置き、当該所属の長をもって充てる。

２　システムセキュリティ責任者の責務

システムセキュリティ責任者は、整備する警察情報システムが必要な情報セキュリティ要件を備えるための事務を処理するものとする。

３　システムセキュリティ責任者の遵守事項

(1)　システムセキュリティ責任者は、整備する警察情報システムの情報セキュリティ要件について、あらかじめ情報セキュリティ管理者の確認を受けなければならない。

(2)　システムセキュリティ責任者は、所管する警察情報システムごとに、当該システムを利用する業務の主管課の長と連携の上、当該システムの運用要領を策定するなどして、当該システムを取り扱う際に遵守すべき事項を職員に周知するとともに、情報セキュリティ管理者に通知しなければならない。この場合において、遵守すべき事項には、次に掲げる事項を含むものとする。

ア　当該システムにおいて取り扱うことのできる情報の機密性の分類の範囲

イ　当該システムにおいて、職員が独自の判断で行うことのできる改造（新たな機器の接続、ソフトウェアの追加等）の範囲

(3)　システムセキュリティ責任者は、所管する警察情報システムについて、情報セキュリティに係る脆（ぜい）弱性に関する情報（以下「脆弱性情報」という。）を入手したときは、情報セキュリティ管理者に報告するとともに、当該脆弱性情報が警察情報システムにもたらすリスクを分析した上で、対策を講じなければならない。この場合において、情報セキュリティ管理者は、当該脆弱性情報が警察庁のシステムと接続された警察情報システムに係るものである場合は、警察庁情報セキュリティ管理者に連絡するものとする。

(4)　システムセキュリティ責任者は、所管する警察情報システムについて、災害時等においても継続して運用できるよう十分検討し、必要に応じて業務継続計画を策定しなければならない。

また、当該業務継続計画は、可能な限り警察情報セキュリティポリシーとの整合を図らなければならない。

(5)　システムセキュリティ責任者は、所管する警察情報システムの情報セキュリティ対策について見直しを行う必要性の有無を適宜検討し、必要があると認めた場合にはその見直しを行い、必要な措置をとらなければならない。

第６　システムセキュリティ維持管理者

１　システムセキュリティ維持管理者の設置

警察情報システムを構成する電子計算機及びネットワーク機器の管理者権限を保有する所属に、システムセキュリティ維持管理者を置き、それぞれ当該所属の長をもって充てる。

２　システムセキュリティ維持管理者の責務

システムセキュリティ維持管理者は、システムセキュリティ責任者の指示等を受け、担当する警察情報システムの維持管理のための事務を処理するものとする。

３　システムセキュリティ維持管理者の遵守事項

(1)　システムセキュリティ維持管理者は、管理者権限を適正に運用しなければならない。

(2)　システムセキュリティ維持管理者は、各種ソフトウェアのうち、利用しない機能は無効化しなければならない。

(3)　システムセキュリティ維持管理者は、脆弱性情報に係る対策、導入したソフトウェアのバージョンアップ等の状況を記録し、定期的にこれを確認及び分析するとともに、不適切な状態にある電子計算機及びネットワーク機器を把握した場合には適切に対処しなければならない。

(4)　システムセキュリティ維持管理者は、警察情報セキュリティポリシー又は当該システムの運用要領に違反する行為を認知したときは、速やかにシステムセキュリティ責任者に連絡しなければならない。

第７　システム管理担当者

１　システム管理担当者の設置

システムセキュリティ維持管理者は、その管理するシステムごとにシステム管理担当者を指名し、業務の責務に即した必要な範囲において、管理者権限を付与しなければならない。

２　システム管理担当者の責務

システム管理担当者は、担当するシステムに係るシステム管理に関する業務を行うものとする。

３　システム管理担当者の遵守事項

(1)　システム管理担当者は、権限のない者にＩＤを発行してはならない。

(2)　システム管理担当者は、警察情報システムに係るドキュメントを適正に管理しなければならない。

(3)　システム管理担当者は、管理対象となる電子計算機に関連する脆弱性情報の入手に努めなければならない。

また、情報を入手した場合には、システムセキュリティ責任者及びシステムセキュリティ維持管理者に報告しなければならない。

(4)　システム管理担当者は、クラス３に指定された区域に設置されている警察情報システムを構成する機器、外部記録媒体及びシステムドキュメントを、クラス２以下に指定された区域に持ち出すときは、その状況を記録しなければならない。

(5)　システム管理担当者は、システムの構成の変更等の作業（軽微なものを除く。）を行う場合において、情報セキュリティの観点から、あらかじめその影響を確認するとともに、その作業を監視し、必要な対応を行わなければならない。

第８　ネットワーク管理担当者

１　ネットワーク管理担当者の設置

システムセキュリティ維持管理者は、その管理するネットワークごとにネットワーク管理担当者を指名し、業務の責務に即した必要な範囲において、管理者権限を付与しなければならない。

２　ネットワーク管理担当者の責務

ネットワーク管理担当者は、担当するネットワーク機器に係るネットワーク管理に関する業務を行うものとする。

３　ネットワーク管理担当者の遵守事項

(1)　ネットワーク管理担当者は、管理対象となるネットワーク機器に関連する脆弱性情報の入手に努めなければならない。

また、情報を入手した場合には、システムセキュリティ責任者及びシステムセキュリティ維持管理者に報告しなければならない。

(2)　ネットワーク管理担当者は、担当するネットワーク機器について、データ伝送に関する監視及び制御を行わなければならない。

(3)　ネットワーク管理担当者は、ネットワークの構成の変更等の作業（軽微なものを除く。）を行う場合において、情報セキュリティの観点から、あらかじめその影響を確認するとともに、その作業を監視し、必要な対応を行わなければならない。

第９　運用管理担当者及び運用管理補助者

１　運用管理担当者

(1)　外部記録媒体又はモバイル端末を利用する所属の運用管理者は、警察本部の課長補佐（室長補佐、隊長補佐及び科長を含む。）、さいたま市警察部若しくは各方面本部の補佐官、警察学校の校長補佐又は警察署の課長（課長代理及び係長制の場合の係長を含む。）以上の職にある職員又は埼玉県警察処務規程（昭和38年埼玉県警察本部訓令第12号）第32条に規定する総括管理者から、運用管理担当者を指名するものとする。

(2)　運用管理担当者は、外部記録媒体の管理及びモバイル端末の持ち出しに関する管理を行うものとする。

２　運用管理補助者

(1)　運用管理者は、運用管理担当者による外部記録媒体の管理が困難な場合は、係長以上の職にある職員から、運用管理補助者を指名することができる。

(2)　運用管理補助者は、運用管理担当者の指示のもと、外部記録媒体の管理を補助するものとする。

一部改正〔平成27年第600号〕

第10　埼玉県警察ＣＳＩＲＴ

1　ＣＳＩＲＴの設置

埼玉県警察本部に、埼玉県警察ＣＳＩＲＴ（以下「ＣＳＩＲＴ」という。）を置く。

2　ＣＳＩＲＴの任務

ＣＳＩＲＴは、警察情報システムに対する不正プログラム感染等の情報セキュリティインシデントが発生した場合に、迅速、的確かつ組織的に対処することを任務とする。

3　ＣＳＩＲＴの体制等

(1)　ＣＳＩＲＴの長は、情報セキュリティ管理者をもって充てる。

(2)　ＣＳＩＲＴの運営に関し必要な事項は、ＣＳＩＲＴの長が関係所属の長と協議して定めるものとする。

(3)　情報セキュリティインシデントが発生した際の措置については、別に定める。

第11　その他

1　分庁舎等における事務

区域情報セキュリティ管理者、システムセキュリティ責任者、システムセキュリティ維持管理者及び運用管理者は、それぞれの事務のうち分庁舎等において処理されるものについて、当該分庁舎等に勤務する警視以上の階級の警察官又はこれと同等の職にある一般職員に担当させることができる。

2　許可等の権限

(1)　許可等の権限を有する者は、自らに対して当該許可等の申請を行ってはならない。

(2)　前記(1)において許可等の申請を行う者は、当該許可等の権限を有する者の上職者に申請を行うことができる。この場合において、当該上職者は、当該許可等に係る所要の措置をとらなければならない。

3　警察情報セキュリティポリシーの見直し

警察情報セキュリティポリシーの規定については、見直しを行う必要性の有無を適宜検討し、必要があると認めた場合にはその見直しを行わなければならない。

実施日

この通達は、平成26年４月１日から実施する。

実施日（平成27年３月24日情管第600号）

この通達は、平成27年４月１日から実施する。